

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 1 1 月 1 9 日
Date of Application:

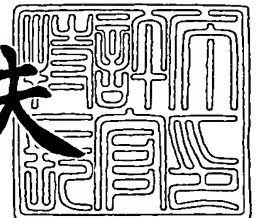
出 願 番 号 特 願 2 0 0 3 - 3 8 9 4 7 5
Application Number:
[ST. 10/C] : [J P 2 0 0 3 - 3 8 9 4 7 5]

出 願 人 株式会社日立製作所
Applicant(s):

2 0 0 4 年 2 月 1 7 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願
【整理番号】 HK15230000
【提出日】 平成15年11月19日
【あて先】 特許庁長官 殿
【国際特許分類】 G06F 12/00
【発明者】
 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1099番地 株式会社日立製作所
 システム開発研究所内
 【氏名】 古川 博
【発明者】
 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1099番地 株式会社日立製作所
 システム開発研究所内
 【氏名】 赤川 悦太郎
【特許出願人】
 【識別番号】 000005108
 【氏名又は名称】 株式会社 日立製作所
【代理人】
 【識別番号】 110000198
 【氏名又は名称】 特許業務法人湘洋内外特許事務所
 【代表者】 三品 岩男
 【電話番号】 045(316)3711
【手数料の表示】
 【予納台帳番号】 221535
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1

【書類名】 特許請求の範囲**【請求項 1】**

ホスト計算機と通信回線を介して接続される記憶装置であって、
前記通信回線に接続するためのインタフェースを備え、
前記インタフェースは、前記通信回線から通信パケットを受信した際、当該通信パケットの中から前記記憶装置へのアクセス用として予め定められたフォーマットの通信パケットであるか否かを判別する第一のフィルタ手段を備えること
を特徴とする記憶装置。

【請求項 2】

請求項 1 記載の記憶装置であって、
前記インタフェースは、前記第一のフィルタ手段において、前記アクセス用と判別された前記通信パケットを受け取り、前記記憶装置内の記憶領域へのアクセスが許可された前記ホスト計算機から送信された通信パケットであるか否かを判別する第二のフィルタ手段をさらに備えること
を特徴とする記憶装置。

【請求項 3】

請求項 2 記載の記憶装置であって、
前記インタフェースは、前記ホスト計算機が前記記憶装置にアクセスが許可されている場合、当該ホスト計算機を一意に特定する情報と、当該ホスト計算機がアクセスを許可されている前記記憶装置内の記憶領域を特定する情報と、を備えたアクセス許可テーブルをさらに備え、
前記第二のフィルタ手段は、前記アクセス許可テーブルに格納された情報に従い、前記アクセス用と判別された通信パケットが、アクセスが許可されたホスト計算機から送信されたものであるか否かを判別すること
を特徴とする記憶装置。

【請求項 4】

請求項 1、2、および、3 いずれか一項記載の記憶装置であって、
前記インタフェースは、
当該インタフェースにおいて受信した全ての通信パケットの通信量と、前記第一のフィルタ手段において前記フォーマットの通信パケットでないものと判定された通信パケットの通信量とをそれぞれ測定し、両通信量を用いて、通信障害が発生しているか否かを判定する通信障害判定手段と、
前記通信障害判定手段において、通信障害が発生していると判断された場合、当該記憶装置に接続され、通知を受けた情報を表示する機能を備える管理サーバに通知する通信障害通知手段とをさらに備えること
を特徴とする記憶装置。

【請求項 5】

請求項 4 記載の記憶装置であって、
前記通信障害判定手段は、前記第二のフィルタ手段において前記アクセスが許可されたホスト計算機から送信された通信パケットでないものと判別された通信パケットの通信量をさらに測定し、当該通信量と前記全ての通信パケットの通信量とを用いて、通信障害が発生しているか否かを、さらに判定すること
を特徴とする記憶装置。

【請求項 6】

請求項 5 に記載の記憶装置であって、
前記インタフェースは、
前記第一のフィルタ手段において前記フォーマットの通信パケットでないものと判別された通信パケットおよび前記前記第二のフィルタで前記アクセスが許可されたホスト計算機から送信された通信パケットでないものと判別された通信パケットの通信情報を、通信ログとして記録する通信ログ記録手段をさらに備えること

を特徴とする記憶装置。

【請求項 7】

請求項 4 ～ 6 いずれか一項記載の記憶装置に接続された管理サーバであって、

前記記憶装置の通信障害通知手段から通信障害が発生していると通知を受けた場合、前記通信ログを参照し、通信障害を発生させている前記通信パケットの発信元を抽出する発信元抽出手段を備えること

を特徴とする管理サーバ。

【請求項 8】

請求項 7 記載の管理サーバであって、

前記発信元抽出手段で抽出された発信元の情報を元に、当該発信元からの通信を遮断するように前記通信回線上に備えられた前記記憶装置への通信を中継する中継装置を制御する中継装置制御手段をさらに備えること

を特徴とする管理サーバ。

【請求項 9】

ホスト計算機と通信回線を介して接続される記憶装置に搭載されるコンピュータを、

前記通信回線に接続するためのインタフェース手段と、

前記通信回線から前記インタフェース手段を介して通信パケットを受信した際、当該通信パケットの中から前記記憶装置へのアクセス用として予め定められたフォーマットの通信パケットであるか否かを判別する第一のフィルタ手段として機能させるためのプログラム。

【請求項 10】

ホスト計算機と通信回線を介して接続される記憶装置に搭載されるコンピュータを、

前記通信回線に接続するためのインタフェース手段と、

前記通信回線から前記インタフェース手段を介して通信パケットを受信した際、当該通信パケットの中から前記記憶装置へのアクセス用として予め定められたフォーマットの通信パケットであるか否かを判別する第一のフィルタ手段と、

前記第一のフィルタ手段において、前記アクセス用と判別された前記通信パケットを受け取り、前記記憶装置内の記憶領域へのアクセスが許可された前記ホスト計算機から送信された通信パケットであるか否かを判別する第二のフィルタ手段と

して機能させるためのプログラム。

【請求項 11】

ホスト計算機と通信回線を介して接続される記憶装置に搭載されるコンピュータを、

前記通信回線に接続するためのインタフェース手段と、

前記通信回線から前記インタフェース手段を介して通信パケットを受信した際、当該通信パケットの中から前記記憶装置へのアクセス用として予め定められたフォーマットの通信パケットであるか否かを判別する第一のフィルタ手段と、

前記インタフェース手段において受信した全ての通信パケットの通信量と、前記第一のフィルタ手段において前記フォーマットの通信パケットでないものと判別された通信パケットの通信量とをそれぞれ測定し、両通信量を用いて、通信障害が発生しているか否かを判定する通信障害判定手段と、

前記通信障害判定手段において、通信障害が発生していると判断された場合、当該記憶装置に接続され、通知を受けた情報を表示する機能を備える管理サーバに通知する通信障害通知手段と、

して機能させるためのプログラム。

【請求項 12】

記憶装置と接続される管理サーバに搭載されるコンピュータを、

前記記憶装置から通信障害が発生していることを示す通知を受けた場合、当該記憶装置が保持する通信ログを参照し、前記通信障害を発生させている通信パケットの発信元を抽出する発信元抽出手段と

して機能させるためのプログラム。

【請求項 13】

記憶装置と接続される管理サーバに搭載されるコンピュータを、

前記記憶装置から通信障害が発生していることを示す通知を受けた場合、当該記憶装置が保持する通信ログを参照し、前記通信障害が発生させている通信パケットの発信元を抽出する発信元抽出手段と、

前記発信元抽出手段で抽出された発信元の情報を元に、当該発信元からの通信を遮断するように、前記記憶装置が通信パケットを受け取るために接続されている通信回線上に備えられた前記記憶装置への通信を中継する中継装置を制御する中継装置制御手段と

して機能させるためのプログラム。

【請求項 14】

請求項 9～13 いずれか一項記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 15】

記憶装置とホスト計算機と管理サーバとが通信回線により接続される記憶装置システムであって、

前記記憶装置は、前記通信回線に接続するためのインタフェースを備え、

前記インタフェースは、

前記通信回線から通信パケットを受信した際、当該通信パケットの中から前記記憶装置へのアクセス用として予め定められたフォーマットの通信パケットであるか否かを判別する第一のフィルタ手段と、

前記第一のフィルタ手段において、前記アクセス用と判別された前記通信パケットを受け取り、前記記憶装置内の記憶領域へのアクセスが許可された前記ホスト計算機から送信された通信パケットであるか否かを判別する第二のフィルタ手段と、

当該インタフェースにおいて受信した全ての通信パケットの通信量および前記第一のフィルタ手段において前記フォーマットの通信パケットでないものと判定された通信パケットの通信量をそれぞれ測定し、両通信量を用いて、通信障害が発生しているか否かを判定する通信障害判定手段と、

前記通信障害判定手段において、通信障害が発生していると判断された場合、前記管理サーバに通知する通信障害通知手段と、

前記第一のフィルタ手段において前記フォーマットの通信パケットでないものと判定された通信パケットおよび前記第二のフィルタ手段において前記アクセスが許可された前記ホスト計算機から送信された通信パケットでないものと判別された通信パケットの通信ログを記録する通信ログ記録手段と、

を備え、

前記管理サーバは、

前記通信障害通知手段から受けた通知を表示する表示手段と、

前記通信障害通知手段から通信障害が発生していると通知を受けた場合、前記通信ログを参照し、通信障害が発生させている前記通信パケットの発信元を抽出する発信元抽出手段と、

前記発信元抽出手段で抽出された発信元の情報を元に、当該発信元からの通信を遮断するように前記通信回線上に備えられた前記記憶装置への通信を中継する中継装置を制御する中継装置制御手段と、を備えること

を特徴とする記憶装置システム。

【請求項 16】

請求項 15 記載の記憶装置システムであって、

前記インタフェースは、前記ホスト計算機が前記記憶装置にアクセスが許可されている場合、当該ホスト計算機を一意に特定する情報と、当該ホスト計算機がアクセスを許可されている前記記憶装置内の記憶領域を特定する情報と、を備えたアクセス許可テーブルをさらに備え、

前記第二のフィルタは、前記アクセス許可テーブルに格納された情報に従い、前記アク

セス用と判別された通信パケットが、アクセスが許可されたホスト計算機から送信されたものであるか否かを判別すること

を特徴とする記憶装置システム。

【請求項 17】

請求項 15 または 16 記載の記憶装置システムであって、

前記通信障害判定手段は、前記第二のフィルタ手段において前記アクセスが許可された前記ホスト計算機から送信された通信パケットでないと判別された通信パケットの通信量をさらに測定し、当該通信量と前記全ての通信パケットの通信量とを用いて、通信障害が発生しているか否かを、さらに判定すること

を特徴とする記憶装置システム。

【請求項 18】

請求項 17 記載の記憶装置システムであって、

前記通信障害判定手段は、前記第二のフィルタ手段において前記アクセスが許可された前記ホスト計算機から送信された通信パケットと判別された通信パケットの通信量をさらに測定し、当該通信量と前記全ての通信パケットの通信量とを用いて、前記アクセスが許可されたホスト計算機から送信された通信パケットの通信量の全通信パケットの通信量に対する比の値が所定以下であるか否かを判別し、

前記通信障害通知手段は、前記通信障害判定手段において、当該比の値が所定以下と判別された場合、第二の通信障害が発生していることを示す通知を前記管理サーバに通知し

、

前記管理サーバは、

前記通信障害通知手段から第二の通信障害が発生していることを示す通知を受けた場合、予め管理者により設定されている前期記憶装置と前記ホスト計算機との間の通信帯域を再調整する帯域調整手段、をさらに備えること

を特徴とする記憶装置システム。

【請求項 19】

記憶装置とホスト計算機と管理サーバとが通信回線により接続される記憶装置システムにおける通信制御方法であって、

前記記憶装置が通信回線からの通信パケットを受信した際、当該通信パケットの中から前記記憶装置へのアクセス用として予め定められたフォーマットの通信パケットであるか否かを判別する第一のフィルタリングステップと、

前記記憶装置が受信した全ての通信パケットの通信量および前記第一のフィルタリングステップにおいて前記フォーマットの通信パケットでないと判別された通信パケットの通信量をそれぞれ測定し、両通信量を用いて、通信障害が発生しているか否かを判定するとともに、前記第一のフィルタリングステップにおいて前記フォーマットの通信パケットでないと判別された通信パケットの通信ログを記録する通信障害判定ステップと、

前記通信障害判定ステップにおいて、通信障害が発生していると判断された場合、前記管理サーバに通知する通信障害通知ステップと、

前記記憶装置から通信障害が発生していると通知を受けた場合、前記通信ログを参照し、当該通信障害を発生させている前記通信パケットの発信元を抽出する発信元抽出ステップと、

前記発信元抽出ステップで抽出された発信元の情報を元に、当該発信元からの通信を遮断するよう前記通信回線上に備えられた前記記憶装置への通信を中継する中継装置を制御する中継装置制御ステップと、を備えること

を特徴とする通信制御方法。

【書類名】明細書

【発明の名称】記憶装置、記憶装置システム、および、通信制御方法

【技術分野】

【0001】

本発明は、ホスト計算機と記憶装置との間の通信に関する。特に、前記ホスト計算機から前記記憶装置内の論理ユニットへのアクセス時の通信におけるフィルタリング技術および通信遮断技術に関する。

【背景技術】

【0002】

1以上のホスト計算機と1以上の記憶装置とをネットワークで接続したストレージシステムにおいて、ホスト計算機から記憶装置内の論理ユニットLU (Logical Unit) へアクセスする際の不正アクセスを防止するセキュリティ技術がある。一例として、ホスト計算機毎にアクセス可能な論理ユニットを制限している環境において、発信元のホスト計算機に関する情報によって受け取った情報のアクセス可否を判断するフィルタリング機能を記憶装置側に備えることで不正なアクセスの遮断を実現しているものがある (例えば、特許文献1参照。)

【0003】

特許文献1に開示されているストレージシステムは、記憶装置内の不揮発メモリ上に、ホスト計算機を一意に識別する情報であるWWN (World Wide Name) と、前記ホスト計算機からのアクセスを許可した記憶装置内の論理ユニットの番号であるLUN (Logical Unit Number) と、前記LUNに対応してユーザやホスト計算機上のオペレーティングシステムが任意に割当てた仮想的なLUの番号である仮想LUNとを対応づけて管理するLUNアクセス管理テーブルに加え、前記ホスト計算機が前記記憶装置にアクセスする際の通信において、ログイン時に動的に割当てられ、前記ホスト計算機が稼働している間は常に一定である管理番号であるS-ID (Source ID) と、前記ホスト計算機のWWNとを対応づけて管理するWWN-S-ID管理テーブルを持つ。

【0004】

特許文献1に開示されているストレージシステムでは、これらの2つの管理テーブルを参照することにより、論理ユニットに対するアクセスの可否を、ログイン時の問合せコマンド発生時点で判断し、以後、この判定を繰り返す必要がない。このため、記憶装置を高い性能で維持運用しながら、論理ユニット単位でアクセス可否を制限でき、強固なセキュリティを実現している。

【0005】

ただし、特許文献1に開示されているストレージシステムは、ファイバチャネル (Fibre Channel; FC) という専用のインタフェースを用いてホスト計算機と記憶装置とを接続してネットワーク化したSAN (Storage Area Network) などの、専用ネットワークにより構築されたシステムである。このため、記憶装置へは、ホスト計算機から記憶装置へのアクセス用のコマンドセットであるSCSIコマンドのみが送信されてくるのが前提である。

【0006】

一方、近年、SCSIコマンドを、IPネットワーク上で送受信するためのプロトコルであるiSCSIの標準仕様が、標準化団体IETFにて検討されている。

【0007】

iSCSIでは、SCSIコマンド等を、IPパケットのペイロードに格納されているTCPパケットの伝送フレームの中に格納 (カプセル化) してIPネットワーク上を流すことにより、コマンドの送受を行い、ホスト計算機と記憶装置との間のI/O処理を実現する。

【0008】

iSCSIを用いることにより、ホスト計算機だけでなく記憶装置も直接IPネットワ

ークに直結でき、従来からIPネットワークで用いられていた、ネットワーク網を構築するハブやルータ、スイッチ類などもそのまま使用できる。

【0009】

従って、IPネットワークを利用して、これまでコスト面や通信距離限界といった技術面から実現が難しかった記憶装置アクセスの広域化に容易に対応できるとともに、成熟しているIPネットワーク管理技術がそのまま適用でき、管理の簡素化も期待できる。

【0010】

【特許文献1】特開2001-265655号公報

【発明の開示】

【発明が解決しようとする課題】

【0011】

しかしながら、前記のiSCSIには、上述のようなメリットがある反面、デメリットも存在する。

【0012】

IPネットワーク上では、多種多様な通信パケットが送受信されている。このため、これまでのホスト計算機と記憶装置との間の専用ネットワークであるFCネットワークで接続されていた場合に比べ、トラフィック通信性能などを予測できない面がある。

【0013】

また、IPネットワークは、全世界に張り巡らされているため、悪意を持った利用者が、IPネットワークに接続された記憶装置等を対象に、システムダウン、データ改竄、窃盗などを目的とした通信攻撃を仕掛けてくる可能性もあり、セキュリティ面で脆弱性を抱えている。

【0014】

特許文献1に開示されているフィルタリング機能は、記憶装置内のいずれかの論理ユニットにアクセスが許可されているパケットのみを通す。このため、基本的にアクセスが許可されていないパケットは、論理ユニットには到達しない。

【0015】

しかしながら、上述したように、特許文献1のフィルタリング機能は、あくまでも記憶装置アクセス用のパケットのみが存在するネットワークを前提に考えられたものであり、IPネットワークのように想定外のパケットが送信されてくるといった環境を意識した作りではない。

【0016】

また、特許文献1に開示されている技術では、アクセスが許可されていないと判断されたパケット（以後、不正なパケットと呼ぶ）は処理されずに廃棄されるだけである。

【0017】

例えば、不正なパケットとしては、その記憶装置にはアクセスが許可されていないホスト計算機からのパケット、そもそも記憶装置自体にアクセスが許可されていない未知の装置からの想定外のパケット、などが考えられる。しかしながら、特許文献1に開示されている技術では、これらの不正なパケットの種別も発信元も判別できない。

【0018】

IPネットワークなどの記憶装置へのアクセス用のパケット以外も送受信されるような通信回線に接続されている環境では、特に、上記の未知の装置からのパケットに、通信攻撃を意図した悪意を持ったパケットが含まれている可能性が高いが、特許文献1に開示されている技術では、このような通信攻撃に対する積極的な防御対策は考慮されていない。

【0019】

本発明は、このような状況に鑑みてなされたもので、通信回線に接続された記憶装置において、セキュリティを高めるとともに、記憶装置への通信帯域を確保することを目的とする。

【課題を解決するための手段】

【0020】

上記目的を達成するために、本発明の記憶装置は、ネットワークからセッション確立時に受信したパケットのうち、正当なパケットのみを記憶装置の論理ユニットに通過させるフィルタリング手段を備える。その際、廃棄するパケットのヘッダ情報等を管理サーバに通知する。通知を受けた管理サーバは、当該ヘッダ情報等を利用して、ネットワーク上の通信を制御する。

【0021】

例えば、本発明は、ホスト計算機と通信回線を介して接続される記憶装置であって、前記通信回線に接続するためのインタフェースを備え、前記インタフェースは、前記通信回線から通信パケットを受信した際、当該通信パケットの中から前記記憶装置へのアクセス用として予め定められたフォーマットの通信パケットであるか否かを判別する第一のフィルタ手段を備えることを特徴とする記憶装置を提供する。

【0022】

また、前記記憶装置は、当該インタフェースにおいて受信した全ての通信パケットの通信量と、前記第一のフィルタ手段において前記フォーマットの通信パケットでないものと判定された通信パケットの通信量とをそれぞれ測定し、両通信量を用いて、通信障害が発生しているか否かを判定する通信障害判定手段と、前記通信障害判定手段において、通信障害が発生していると判断された場合、当該記憶装置に接続され、通知を受けた情報を表示する機能を備える管理サーバに通知する通信障害通知手段とをさらに備え、前記管理サーバは、前記通信障害通知手段から通信障害が発生していると通知を受けた場合、前記通信ログを参照し、通信障害を発生させている前記通信パケットの発信元を抽出する発信元抽出手段と、前記発信元抽出手段で抽出された発信元の情報を元に、当該発信元からの通信を遮断するよう前記通信回線上に備えられた前記記憶装置への通信を中継する中継装置を制御する中継装置制御手段とを備える。

【発明の効果】

【0023】

本発明によれば、通信回線に接続された記憶装置において、セキュリティを高めることができる。さらに、記憶装置への通信帯域を確保できる。

【発明を実施するための最良の形態】

【0024】

以下、本発明の一実施形態を、図面を用いて説明する。

【0025】

ここで、本実施形態では、1以上のホスト計算機と1以上の記憶装置とを備えるストレージシステムにおいて、記憶装置とホスト計算機との間の通信にiSCSIを用いる場合を例にあげて説明する。すなわち、本実施形態では、両者間で使用するプロトコルとして、ネットワーク層のプロトコルはIP（Internet Protocol）であり、トランスポート層のプロトコルはTCP（Transmission Control Protocol）であるTCP/IPを用い、記憶装置の制御を実施するコマンドセットとして、SCSIコマンドを用いる。SCSIコマンドは、TCP/IP上をやりとりするパケット内にカプセル化されて送受信される。

【0026】

もちろん、本発明は、前述のプロトコルやコマンドセットに限定されるものでなく、ホスト計算機から記憶装置にアクセスするためのコマンドセットを、ネットワークで用いられているプロトコル上に実装している仕様であれば、その形式は問わない。

【0027】

本実施形態の前提である、iSCSIの構成と送受信されるパケットの概念図を図1に示す。本図において、100は記憶装置、200はホスト計算機、300は記憶装置100とホスト計算機200との間を接続するIPネットワークである。また、本実施形態では、IPネットワーク上を送受信されるIPパケットの中で、IPパケットのペイロードに格納されているTCPパケットにSCSIコマンド、SCSIレスポンス等を格納した

ものを、iSCSI パケット 310 と呼ぶ。

【0028】

iSCSI プロトコルでは、SCSI コマンド 311 の発行元を iSCSI イニシエータと呼び、受け取ったコマンドを処理して SCSI コマンド 311 に対するレスポンス 312 を返す側を iSCSI ターゲットと呼ぶ。従って、本図では、ホスト計算機 200 が iSCSI イニシエータ、記憶装置 100 が iSCSI ターゲットとなる。

【0029】

iSCSI の階層モデルでは、iSCSI 層は、SCSI コマンドをやりとりする SCSI 層と TCP/IP 層との間に位置する。iSCSI 層は、SCSI 層から SCSI コマンド等を受け取り、それをカプセル化して SCSI PDU (Protocol Data Unit) を作成し、TCP/IP 層に受け渡す。また、TCP/IP 層から受け取った iSCSI PDU を処理して、SCSI コマンド等を取り出し、それを SCSI 層に受け渡す。

【0030】

iSCSI パケット 310 の TCP/IP 層以下の通信データ構成は、一般的な TCP/IP パケット構成と同様であり、iSCSI パケット 310 は、カプセル化された SCSI コマンドを処理するまでは、通常の TCP/IP パケットとして IP ネットワーク 300 上を送受信される。

【0031】

なお、iSCSI パケット 310 のヘッダには、当該パケットに iSCSI コマンドがカプセル化されていることを示す情報が含まれる。このため、iSCSI パケットを受け取った iSCSI ターゲット側では、TCP/IP 層において iSCSI コマンドを取り出す処理を行わなくても、ヘッダ情報を確認することで、当該パケットが、iSCSI パケット 310 であるか否かを判別できる。

【0032】

また、iSCSI では、iSCSI 層において、iSCSI イニシエータ 200 と iSCSI ターゲット 100 との間に論理的な通信路であるセッションを確立して通信を行なう。セッションは TCP 層の一般的なコネクションの確立の手续と同様に、認証を得て確立される。認証を得るための手续のことを、iSCSI では iSCSI ログインと呼ぶ。本実施形態では、セッション確立前、すなわち、iSCSI ログイン前の全 IP パケット各々について iSCSI パケットであるか否かをフィルタリングし、iSCSI パケットであれば、セッションを確立する。そして、セッション確立後は、その認証を信頼してパケットのフィルタリングは行わない。

【0033】

なお、これらのセッション確立やログインの方法は、従来の FC ネットワークで接続された記憶装置 100 とホスト計算機 200 との間のものと同様の仕様である(特許文献 1 参照)。従って、SCSI 層から見た場合、下位の階層の種類、すなわち、TCP/IP と FC とによるネットワークの種類による違いは無い。

【0034】

また、特許文献 1 では、ホスト計算機 200 を一意に特定するために、FC フレームヘッダの S-ID から WWN を特定するデータ変換が行われている。iSCSI では、セッション確立時にホスト計算機 200 を特定するために、IP ネットワーク 300 で従来から利用されているドメイン概念の iSCSI ネームを用いる。iSCSI ネームは、iSCSI パケットのヘッダ情報に含まれる。

【0035】

以上により、iSCSI による記憶装置 100 とホスト計算機 200 とのネットワーク接続とは、これまで FC ネットワークで構成されていたものが IP ネットワーク 300 に取って代わっただけで、記憶装置へのアクセス仕様には全く違いがないことがわかる。

【0036】

次に、本実施形態のストレージシステムについて説明する。図 2 は、本実施形態のストレージシステムの機能構成図である。

【0037】

本図に示すように、本実施形態のストレージシステムは、1以上のホスト計算機200と、1以上の記憶装置100と、管理サーバ400と、IPネットワーク300とを備える。

【0038】

IPネットワーク300は、通信プロトコルにTCP/IPを利用するネットワークで、インターネットに代表されるように現在全世界的に張り巡らされ、様々な情報機器が接続されるネットワーク環境である。記憶装置100とホスト計算機200と管理サーバ400とは、このIPネットワーク300によって接続される。iSCSIパケットも、他のIPパケットと同様に、IPネットワーク300を介してやり取りされる。

【0039】

ここで、本実施形態においては、IPネットワーク300は、ルータもしくはスイッチ320によりスター型に接続される構成を例にあげて説明を行なう。しかし、ネットワーク構成はこれに限られない。記憶装置100とホスト計算機200との間に、ルータもしくはスイッチ320が配置されていればよい。

【0040】

記憶装置100は、記憶装置100外から、IPパケットを受信するストレージ用インタフェース110と、記憶領域である論理ユニット(LU)130と、I/O命令を受けて論理ユニット130の制御を実施する記憶領域制御装置131と、記憶装置100を保守管理する保守用端末150と、該保守用端末150に記憶装置100側の情報を通信する通信制御部161と、I/O処理などの高速化を実現するキャッシュメモリ162とを備える。

【0041】

ここで、ストレージ用インタフェース110は、ハードウェア構成として、全体の動作を統括制御する制御プロセッサ111と、制御プロセッサ111が実行するプログラムを記憶する制御メモリ112と、制御プロセッサ111停止時もデータを格納する不揮発メモリ113と、外部ネットワークとのI/Fであるポート114とを備える。

【0042】

制御プロセッサ111は、制御メモリ112に格納されたプログラムを実行することにより、IPレベルフィルタ部115と、LUレベルフィルタ部116と、通信量測定・判定部117と、通信情報および障害通知部118と、iSCSI処理エンジン119と、の各機能を実現する。

【0043】

不揮発メモリ113には、上記プログラムを実行する際に使用されるLUアクセス許可テーブル121と、通信障害判定用閾値テーブル122とが格納される。

【0044】

IPレベルフィルタ部115は、セッション確立前のIPパケットをフィルタリングする。具体的には、セッション確立前にポート114において受信した全てのIPパケットのヘッダ情報を参照し、iSCSIパケットであることを示す情報が格納されているか否かにより、当該IPパケットがiSCSIパケットであるか否かを判別する。

【0045】

iSCSIパケットと判別された場合、LUレベルフィルタ部116に送出し、その他のIPパケット(以後、非iSCSIパケットと呼ぶ)は、通信量測定・判定部117を介して通信情報および障害通知部118に送出する。

【0046】

LUレベルフィルタ部116は、受け取ったiSCSIパケットをフィルタリングする。具体的には、受け取ったiSCSIパケットが論理ユニット130にアクセス可能か否かを、iSCSIログイン時に受け取ったiSCSIパケットのiSCSIネームに基づいて後述するLUアクセス許可テーブル121を参照し判断する。なお、その後、当該ログインが有効である間は、当該iSCSIネームを有するiSCSIパケットの論理ユニ

ット130へのアクセス可否のチェックは行わない。

【0047】

アクセス可能なiSCSIパケット（以後、許可iSCSIパケットと呼ぶ）は、通信量測定・判定部117を介してiSCSI処理エンジン119に送出する。アクセス許可のないiSCSIパケット（以後、不許可iSCSIパケットと呼ぶ）は、通信量測定・判定部117を介して通信情報および障害通知部118に送出する。

【0048】

ここで、LUアクセス許可テーブル121について説明する。LUアクセス許可テーブル121は、ホスト計算機毎に、アクセスが許可されている論理ユニット130に対応付けて格納したものである。図3にLUアクセス許可テーブル121の一例を示す。

【0049】

本図に示すように、LUアクセス許可テーブル121は、ホスト計算器200を一意に特定するiSCSIネーム1211と、ユーザやホスト計算機200上のオペレーティングシステムが論理ユニット130に任意に割当てた仮想的な論理ユニット番号(仮想LUN)1212と、仮想LUN1212に対応する記憶装置100上で論理ユニット130を一意に特定する論理ユニット番号(LUN)1213とを備える。このLUアクセス許可テーブル121は、管理者などにより予め、管理サーバ400などから設定される。

【0050】

LUレベルフィルタ部116が受け取ったiSCSIパケットのヘッダに格納されているiSCSIネームと同じiSCSIネームが、LUアクセス許可テーブル121のiSCSIネーム1211に格納され、それに対応する仮想LUN1212、LUN1213が格納されていれば、アクセスが許可されていることを意味する。なお、LUレベルフィルタ部116におけるアクセス可否の判定方法については、特許文献1の方法と同様であるため、ここではその説明を省略する。

【0051】

通信量測定・判定部117は、IPレベルフィルタ部115およびLUレベルフィルタ部116の2つのフィルタ手段で分別された3種のパケット（許可iSCSIパケット、不許可iSCSIパケット、非iSCSIパケット）を受け取り、それぞれの単位時間当たりの通信量を測定した後、受け取ったパケットの種類に応じて、通信情報および障害通知部118、または、iSCSI処理エンジン119に送出する。また、単位時間当たりの測定結果を用いて、通信障害判定用閾値テーブル122に従って通信障害発生の有無を判定する。

【0052】

ここで、通信障害判定用閾値テーブル122は、判定対象ごとに、その閾値とともに判断基準が格納されているテーブルである。図4に通信障害判定用閾値テーブル122の一例を示す。

【0053】

本実施形態の通信障害判定用閾値テーブル122は、判定対象通信比の内容を格納する判定対象通信比格納欄122aと、通信障害と判定する閾値とともに判断基準を格納する閾値格納欄122bとを備える。

【0054】

本実施形態では、判定対象通信比として、例えば、非iSCSIパケットの単位時間当たりの通信量がストレージ用インタフェース110において受信した全パケットの単位時間当たりの通信量に対して占める割合1221（以後、非iSCSIパケット比と呼ぶ。）、不許可iSCSIパケットの単位時間当たりの通信量がIPレベルフィルタ部115において判別された全てのiSCSIパケットの単位時間当たりの通信量に対して占める割合1222（以後、不許可iSCSIパケット比と呼ぶ。）、および、許可iSCSIパケットの単位時間当たりの通信量がストレージ用インタフェース110において受信した全パケットの単位時間当たりの通信量に占める割合1223（以後、許可iSCSIパケット比と呼ぶ。）などが格納される。

【0055】

なお、それぞれの比から判定される通信障害とは、例えば、非 i S C S I パケット比の場合、不正なパケットによる通信攻撃によるもの、不許可 i S C S I パケット比の場合、既に記憶装置 100 にアクセス権を有していない状態となったホスト計算機 200 が、何らかの事情で、そのままアクセスを続けていることによるもの、許可 i S C S I パケット比の場合、通信帯域設定が適切でないことによるものである。閾値格納欄 122b には、これらの通信障害の発生が判定できる値および基準が格納される。

【0056】

本実施形態では、通信量測定・判定部 117 は、それぞれの測定結果から得られる通信比の値が、閾値格納欄 122b に格納されている条件を満たす場合、通信障害と判定し、通信障害が発生した旨、通信障害が発生したと判断した通信比の種類（障害種別：非 i S C S I パケット比、不許可 i S C S I パケット比、または、許可 i S C S I パケット比など）、通信障害が発生したと判断した際の通信比の値、通信障害が発生したと判断した通信量を測定した単位時間の時間情報（障害時刻）、および、通信障害が発生したと判断した際のパケットの通信情報を、通信情報および障害通知部 118 に通知する。ここで、通知する通信情報は、後述の通信ログ 158 において説明する。

【0057】

例えば、全パケットの通信量が 150 K B y t e / s の時、非 i S C S I パケットの通信量が 100 K B y t e / s あったとすると、通信障害判定用閾値テーブル 122 の非 i S C S I パケット比 1221 の値は 66 % となり、閾値格納部 122b に格納されている「50 % 以上」に該当する。このような場合、通信量測定・判定部 117 は、i S C S I パケットの正常な通信に問題が出る程度の通信が記憶装置 100 に届いている、すなわち、障害発生と判定する。

【0058】

なお、本図に示す判定対象通信比は一例であり、I P レベルフィルタ部 115 および L U レベルフィルタ部 116 の 2 つのフィルタ手段で判別される 3 つのパケットに関する情報から測定される任意の通信量を用いて得られる各種の通信比を判定対象として用いることが可能である。

【0059】

通信情報および障害通知部 118 は、I P レベルフィルタ部 115 および L U レベルフィルタ部 116 の 2 つのフィルタ部から、通信量測定・判定部 117 を介して受け取ったパケット、および、通信量測定・判定部 117 において通信障害と判定された場合に受け取った情報を保守用端末 150 に送信する。

【0060】

i S C S I 処理エンジン 119 は、I P レベルフィルタ部 115 および L U レベルフィルタ部 116 を経て受け取った許可 i S C S I パケットに対し、i S C S I ターゲットとしての処理を施し、S C S I コマンドを取り出し、送信先として指定された論理ユニット 130 に送信する。

【0061】

なお、上記機能を実現するプログラムは、制御メモリ 112 ではなく、制御プロセッサ 111 が読み取り可能な記録媒体（フレキシブルディスク、CD-ROM、DVD-ROM、半導体メモリ、LAN 及び SAN 等の伝送経路等）に格納されていても良い。また、これらのプログラムは、その機能をハードウェア構成（L S I（Large Scale Integration）等の半導体集積回路等）で実現しても良い。

【0062】

保守用端末 150 は、ハードウェア構成として、保守用端末 150 全体の動作を統括制御する制御プロセッサ 151 と、制御プロセッサ 151 が実行するプログラムを記憶する制御メモリ 152 と、データを記録保存する保守用端末記憶領域 153 と、外部ネットワークとのインタフェース 154 と、記憶装置 100 本体とのインタフェース 155 とを備える。

【0063】

制御プロセッサ151は、制御メモリ152に格納されたプログラムを実行することにより、通信情報記録部156と、警告メッセージ通報部157と、の各機能を実現する。

【0064】

保守用端末記憶領域153には、通信ログ158が記録保存される。

【0065】

通信情報記録部156は、通信情報および障害通知部118から送付されてきたパケットの通信情報を通信ログ158として保守用端末記憶領域153に記録する。

【0066】

ここで、通信ログ158に記録される情報を説明する。図5に本実施形態における通信ログ158の一例を示す。

【0067】

記録されるパケットの通信情報は、例えば、本図に示すように、当該通信情報が記録された日時1581、当該通信のパケットのプロトコルの種類1582、送信元のIPアドレスおよび使用ポート番号1583、送信先のIPアドレスおよび使用ポート番号1584、などである。

【0068】

なお、ここで示す通信ログは一例であり、以上の情報が最低限含まれていれば、その記録形式、および、その他の情報の有無は問わない。

【0069】

警告メッセージ通報部157は、通信情報および障害通知部118から送付されてきた通信障害が発生した旨の通知、障害種別、通信比の値、および、障害時刻の情報をうい、予め障害種別毎に用意されているテキストメッセージと組み合わせて警告メッセージを生成し、管理サーバ400に通報する。

【0070】

なお、これらの機能を実現するプログラムは、制御プロセッサ151により読み取り可能な記録媒体（フレキシブルディスク、CD-ROM、DVD-ROM、半導体メモリ、LAN及びSAN等の伝送経路等）に格納しても良い。

【0071】

また、これらプログラムは、その機能をハードウェア構成（LSI（Large Scale Integration）等の半導体集積回路等）で実現しても良い。

【0072】

なお、本実施形態では、保守用端末150を記憶装置100内に含む構成を例にあげて説明するが、保守用端末150の構成はこれに限られない。例えば、記憶装置100外に備えられる構成であってもよい。また、複数の記憶装置100について、1つの保守用端末150を備えるよう構成してもよい。

【0073】

ホスト計算機200は、ハードウェア構成として、全体の動作を統括制御する制御プロセッサ201と、制御プロセッサ201が実行するプログラムを記憶する制御メモリ202と、外部ネットワークとのインタフェース203とを備える。

【0074】

ホスト計算機200は、制御メモリ202上に、SCSIコマンドを伝送フレームに格納することにより、iSCSIパケットを生成するiSCSIドライバ211を備える。

【0075】

なお、iSCSIドライバ211は、制御プロセッサ201により実行されることによりその機能が実現されるプログラムである。また、このプログラムは、制御プロセッサ201により読み取り可能な記録媒体（フレキシブルディスク、CD-ROM、DVD-ROM、半導体メモリ、LAN及びSAN等の伝送経路等）に格納しても良い。また、これらプログラムは、その機能をハードウェア構成（LSI（Large Scale Integration）等の半導体集積回路等）で実現しても良い。

【0076】

管理サーバ400は、ハードウェア構成として、全体の動作を統括制御する制御プロセッサ401と、制御プロセッサ401が実行するプログラムを記憶する制御メモリ402と、外部ネットワークとのインタフェース403と、入出力装置とのI/F404と、入力装置405と、出力装置406とを備える。

【0077】

制御プロセッサ401は、制御メモリ402に格納されたプログラムを実行することにより、帯域条件指定部411と、障害情報表示部412と、不正通信発生元解析部413と、ルータ・スイッチ制御指示部414との各機能を実現する。

【0078】

障害情報表示部412は、管理サーバ400に記憶装置100から警告メッセージが送付されてきた際に、送付されてきた警告メッセージが示す情報を出力装置406に表示する。

【0079】

帯域条件指定部411は、記憶装置100から警告メッセージが送付されてきた際にIPネットワーク上で確保したい通信帯域の情報を、管理者から入力装置405を介して受け付け、設定する。設定時期は、システムの構築が完了した後、必要に応じて管理者が決定する。例えば、構築直後、あるいは、出力装置406に表示された警告メッセージの内容を見た管理者が再設定が必要と判断した場合などである。

【0080】

さらに、警告メッセージを受け取った際、当該障害種別が、許可iSCSIパケット比1223を示すものであった場合、帯域条件指定部411は、通信障害判定用閾値テーブル122にアクセスし、警告メッセージ内の通信比の値と、通信障害判定閾値テーブル122の対応する通信比の閾値格納欄122bに設定されている最新の閾値および判断基準とを比較し、通信帯域を再調整する必要があるか否かを判断する。

【0081】

具体的な判定例を以下に挙げる。例えば、管理者により、ルータ・スイッチ320が、記憶装置100の論理ユニット130へのアクセスに使用する帯域において、誤差10%未満で、全体通信量の70%をiSCSIパケット用に確保するように制御するように設定されているとする。この場合、通信障害判定用閾値テーブル122には、図4に示すように、正常な制御範囲を超えたか否かを判定する閾値および判断基準として60%以下が設定される。このような設定がなされている時に、許可iSCSIパケット比が60%以下に落ち込んだ場合、すなわち、ルータ・スイッチ320によって、帯域制御が設定どおりになされていない状態になった場合、通信量測定・判定部117によって、障害発生と判定されることにより、その状態が検出され、警告メッセージ通報部157を介して、管理サーバ400に通知がなされる。

【0082】

通常は、通信障害判定用閾値テーブル122の閾値格納欄122bに格納されている判断基準に合致した場合、警告メッセージが発行されるため、警告メッセージが発行されれば、再調整が必要となる。しかし、通信障害判定用閾値テーブル122の閾値および判断基準は、警告メッセージ発生時の値等から変更されていることがありえる。このため、帯域条件指定部411において、一旦判断を行う。

【0083】

そして、判断結果が再調整が必要であるもの、すなわち、通信障害判定用閾値テーブル122に設定されている判断基準に合致するものであった場合は、後述するルータ・スイッチ制御指示部414に向けて、帯域を調整するための制御命令を発行する。

【0084】

ここで、制御命令は、例えば、許可iSCSIパケットのスループットが、ターゲットとしている帯域に近づくよう、ルータ・スイッチの構成を変更するもので、例えば、ルータ・スイッチにおけるキューイング待ち時間等を長くするといったパラメータ値を変更す

るものがある。

【0085】

不正通信発生元解析部413は、管理サーバ400に記憶装置100から警告メッセージが送付されてきた際に、警告メッセージ内の障害時刻の情報を元に、保守用端末の記憶領域153に記録されている通信ログ158にアクセスし、大量に非iSCSIパケットを送信してくるといった通信攻撃と考えられる不正通信の発行元を解析する。

【0086】

具体的な解析例を以下に説明する。例えば、前述の通信量測定・判定部117が、図5に示す通信ログ158群を基に、単位時間として2003年7月15日10:00:01から10:00:02の1秒間の通信量を測定し、閾値を越えているため、障害発生と判断したものとする。ここで、図5に示す通信ログの場合、2003年7月15日10:00:01から10:00:02の間に、非iSCSIパケットが、同じ発信元から多量に届いている。

【0087】

この場合、警告メッセージには、障害時刻として2003年7月15日10:00:01が格納される。不正通信発生元解析部413は、この警告メッセージ内の障害時刻に該当する通信ログ158を抽出する。

【0088】

その中から非iSCSIパケットを抽出し、送信元毎に、通信量を得る。そして、所定の通信量を超えるなどした送信元のアドレス情報1583を抽出する。

【0089】

そして、後述するルータ・スイッチ制御指示部414に向けて、当該不正通信の発行元からの通信を遮断することを指示する制御命令を発行する。

【0090】

ルータ・スイッチ制御指示部414は、管理サーバ400に記憶装置100から警告メッセージが送付されてきた際に、帯域条件指定部411および不正通信発生元解析部413から発行された制御命令に従って、ルータ・スイッチ300を制御し、不正通信の発行元からのパケットを遮断し、正常アクセスのパケットの帯域を確保する。

【0091】

なお、これらの機能を実現するプログラムは、制御プロセッサ401により読み取り可能な記録媒体（フレキシブルディスク、CD-ROM、DVD-ROM、半導体メモリ、LAN及びSAN等の伝送経路等）に格納されても良い。

【0092】

また、これらプログラムは、その機能をハードウェア構成（LSI（Large Scale Integration）等の半導体集積回路等）で実現しても良い。

【0093】

次に、上記の機能を有する本実施形態のストレージシステムにおいて、記憶装置100がパケットを受信した場合の処理流れの概要を説明する。図6は、本実施形態のシステムを構成する要素のうち、処理の概要を説明するために代表的なものを記載した構成図である。

【0094】

ここで、本図において、矢印001～003の向きに送信されるパケットを、それぞれ、パケット001、パケット002、パケット003と呼ぶ。これらは、iSCSIターゲットである記憶装置100に、IPネットワーク300から送信されるパケットである。この中で、パケット001は、許可iSCSIパケット、パケット002は、不許可iSCSIパケット、パケット003は発信元が不明な情報機器から、記憶装置100に向け発信された非iSCSIパケットとする。

【0095】

記憶装置100上のストレージ用インタフェース110は、パケット001、002、003を受信すると、IPレベルフィルタ部115により、受信したパケットを選別する

。ここでは、パケット001およびパケット002がiSCSIパケットと判断され、LUレベルフィルタ部116に向けて送出される。一方、パケット003は、破棄するものとして矢印004に従って、通信量測定・判定部117を介して通信情報および障害通知部118に向けて送出される。通信量測定・判定部117では、パケット003の単位時間当たりの通信量を測定し、必要な通信比を算出し、通信障害判定用閾値テーブル122を参照しながら、通信障害の発生をモニタする。

【0096】

一方、IPレベルフィルタ部115からLUレベルフィルタ部116に向けて送出されたiSCSIパケットであるパケット001および002は、LUレベルフィルタ部116により、LUアクセス許可テーブル121を参照しながら、記憶装置100内論理ユニット130にアクセスが許可されているパケットであるか判断される。

【0097】

そして、LUレベルフィルタ部116は、パケット002を廃棄するものとして、矢印005に従って、通信量測定・判定部117を介して通信情報および障害通知部118に向けて送出する。通信量測定・判定部117では、パケット002の単位時間当たりの通信量を測定し、必要な通信比を算出し、通信障害判定用閾値テーブル122を参照しながら、通信障害の発生をモニタする。

【0098】

一方、LUレベルフィルタ部116は、パケット001を、論理ユニット130にアクセスが許可されているパケットであると判断し、矢印006に従って通信量測定・判定部117を介してiSCSIエンジン119に向けて送出する。iSCSI処理エンジン119においてSCSIコマンドが取り出され、取り出されたiSCSIコマンドが論理ユニット130に送られ、I/O処理が実施される。

【0099】

なお、通信量測定・判定部117では、パケット001の単位時間当たりの通信量を測定し、必要な通信比を算出し、通信障害判定用閾値テーブル122を参照しながら、通信障害の発生をモニタする。

【0100】

通信情報および障害通知部118は、図6の矢印007に従って、パケット002および003の通信情報を記憶装置100内の保守用端末150の通信情報記録部156に送信する。その後、通信情報記録部156は、パケット002および003の通信情報を、通信ログ158として記録する。

【0101】

また、通信量測定・判定部117は、通信障害判定用閾値テーブル122の閾値を利用して、通信障害が発生しているか否か判定する。

【0102】

判定で通信障害が発生していると判断された場合には、図6の矢印008に従って、通信情報および障害通知部118を介して、保守用端末150内の警告メッセージ通報部157に情報が伝達され、図6の矢印009に従って、それを受けた警告メッセージ通報部157が警告メッセージを発信することにより、管理サーバ400にその旨を通報する。

【0103】

警告メッセージを受けた管理サーバ400は、それぞれの通信障害に応じた警告メッセージを表示することにより管理者に情報を提示する。また、警告メッセージに応じた適切な性能低下防止処理を実行する。

【0104】

以下に、警告メッセージが管理サーバ400に送信される処理の流れ、および、警告メッセージを受けた場合に管理サーバ400が行う性能低下防止処理について説明する。

【0105】

図7は、不適切なパケット（不許可iSCSIパケット、非iSCSIパケット）を受信した場合の、本実施形態のストレージシステム内の処理フローを示す。

【0106】

まず、通信量測定・判定部117は、IPレベルフィルタ部115および/またはLUレベルフィルタ部116を経て廃棄（論理ユニット130に送信しない）と判定されたパケット、および、ストレージ用インタフェース110で受信した全パケットについて、単位時間当たり（例えば、1秒）の通信量を測定し、測定した単位時間毎に、予め定めた通信比を算出する（ステップ0100）。

【0107】

次に通信量測定・判定部117は、算出された通信比を基に、通信障害判定用閾値テーブル122を参照し、障害と判定する基準に該当するか否かを判定する（ステップ0110）。

【0108】

ステップ0110で通信障害判定用閾値テーブル122に該当する項目が無い場合（Noの場合）は、ステップ0100に戻り、再度処理を開始する。

【0109】

一方、ステップ0110で通信障害判定用閾値テーブル122に該当する項目がある場合（Yesの場合）は、通信量測定・判定部117は、障害種別（不許可パケット比、または、非iSCSIパケット比）等を、障害通知部118を介して、警告メッセージ通報部157に通知する（ステップ0120）。

【0110】

通知を受けた警告メッセージ通報部157は、障害種別に応じた警告メッセージを生成し、障害情報として管理サーバ400に通報する（ステップ0130）。

【0111】

警告メッセージを受けた管理サーバ400は、障害情報表示部411に、出力装置406に前記障害メッセージの内容を表示させ、管理者に提示する（ステップ0140）。管理者は、表示内容を確認することにより、現在の記憶装置100の通信状態を把握することができ、例えば、帯域の再設定などの処理を行うことができる。

【0112】

管理サーバ400は、上記のように、警告メッセージを受け取った際、その内容を出力装置406に提示することにより、管理者の注意を促し、管理者の対処を受け付けるだけでなく、自ら、受け取った警告メッセージの内容に応じて、ストレージシステムの性能低下防止処理を行うことができる。

【0113】

次に上記のステップ0130において、受け取った警告メッセージが、非iSCSIパケット比が、閾値を超えることを意味するものであった場合、または、不許可iSCSIパケット比が、閾値を超えることを意味するものであった場合、すなわち、不適切なパケットのアクセスが増えた場合、管理サーバ400が行う性能低下防止処理について説明する。ここで、管理サーバ400が行う性能低下防止処理とは、記憶装置のI/O性能低下をもたらしているパケットを遮断することである。

【0114】

なお、本実施形態では、非iSCSIパケット比が閾値を越えた場合を例に、管理サーバ400において、通信ログ158の内容を解析して不正通信の発行元を突き止め、記憶装置100への通信路のIPネットワーク300上にあるルータ、スイッチ320などのIPネットワーク中継器機を制御し、当該不正通信の発行元からの通信を遮断するといった処理を説明する。

【0115】

図8に、不正なアクセスが増えた場合、管理サーバ400においてなされる処理のフローを示す。

【0116】

まず、管理サーバ400は、保守用端末150から、障害種別が非iSCSIパケット比が閾値を超えたことを示す警告メッセージを受け取る（ステップ0200）。

【0117】

警告メッセージを受けた管理サーバ400は、障害情報表示部412にステップ0200で受け取った警告メッセージに応じた表示を出力装置406に表示させるとともに、不正通信発生元解析部413に保守用端末150に記録されている通信ログ158を取得させる(ステップ0210)。

【0118】

不正通信発生元解析部413は取得した通信ログ158の情報をを用いて、該当する通信ログを解析し、不正なパケットの送信元のアドレス情報等を抽出する(ステップ0220)。

【0119】

不正通信発生元解析部413は、該当アドレス1583(例えば、図5の例の場合10.X.X.X)からのパケットを全て遮断する処置を実行するため、ルータ・スイッチ制御指示部414に、当該アドレス1583からの通信を遮断することを意味するルータもしくはスイッチの制御命令を発行する(ステップ0230)。

【0120】

ルータ・スイッチ制御指示部414は、ステップ0230で発行された制御命令に従い、該当アドレスからのパケットを遮断するようルータもしくはスイッチ320を制御する(ステップ0240)。

【0121】

本実施形態のストレージシステムは、上記のような処理を行うことにより、記憶装置100を攻撃対象とした通信攻撃を遮断することができる。

【0122】

次に、上記のステップ130において、受け取った警告メッセージが、正常に論理ユニット130にアクセスするiSCSIパケットの通信量の割合が減ったことを意味するものであった場合、すなわち、許可iSCSIパケット比が閾値以下となった場合の処理について、以下に説明する。

【0123】

ここで、管理サーバ400が行う性能低下防止処理とは、予め管理者により指定されたIPネットワークの帯域制御に関する指示に基づき、許可iSCSIパケットに、必要な帯域を確保することである。管理サーバ400が、記憶装置100への通信路のIPネットワーク300上にあるルータ、スイッチ320などのIPネットワーク中継器機を制御し、記憶装置100にアクセス権限のあるホスト計算機200からのアクセスのために必要な帯域を確保する。

【0124】

図9に、許可iSCSIパケット比が閾値以下となった場合、管理サーバ400においてなされる処理のフローを示す。

【0125】

まず、管理サーバ400は、保守用端末150から、許可iSCSIパケット比が閾値以下となったことを示す警告メッセージを受け取る(ステップ0300)。

【0126】

警告メッセージを受け取った管理サーバ400は、障害情報表示部412に受け取った警告メッセージの内容に応じた表示を表示装置406に表示させるとともに、帯域制御条件指定部411に警告メッセージに含まれる情報を通知する(ステップ0310)。

【0127】

帯域制御条件指定部411は、通信障害判定用閾値テーブル122の閾値格納欄122bに格納されている値と、警告メッセージによって受け取った通信量比の値とを比較し、帯域制御の設定が妥当なものかどうか、つまり再調整が必要かを判定する(ステップ0320)。

【0128】

ステップ0320における判定で帯域制御の再調整が必要と判断された場合(Yesの

場合)、ルータ・スイッチ制御指示部 414 に、与えられた帯域制御を実施するために必要な命令を送付する (0330)。

【0129】

一方、再調整が必要ないと判断された場合 (No の場合)、処理を終了する。

【0130】

ステップ 0330 で命令を受けたルータ・スイッチ制御指示部 414 は、ルータのコマンド等で指定された条件の帯域制御設定を再調整し (0340)、処理を終了する。

【0131】

本実施形態のストレージシステムは、上記のような処理を行うことにより、通信状態に応じて、記憶装置 100 に対する帯域設定を動的に再調整することが可能となる。

【0132】

このように、本実施形態によれば、ストレージシステムは、記憶装置 100 において、論理ユニット 130 にアクセス可能なパケット (正常なパケット) とそれ以外のパケット (不正なパケット) とを振り分けることができる。

【0133】

本実施形態では、この振り分けを、受け取ったパケットから、iSCSI パケットのみを抽出する IP レベルフィルタ (第一のフィルタ) と、iSCSI パケットから記憶装置にアクセスが許可されているパケットのみを抽出する LU レベルフィルタ (第二のフィルタ) との 2 つのフィルタにより実現している。しかも、LU レベルフィルタでのアクセス可否の判断は、セッションの確立時、すなわち、iSCSI ログイン時に送信される iSCSI パケットのみで行われる。そして、当該パケットによりセッションが確立した後は、個々のパケットのアクセスの可否を判断しない。このため、効率よくアクセスの可否を判断できる。

【0134】

また、不正なパケットと振り分けられたものの通信ログを記録しているため、当該情報を用いて、今後の受信を遮断する措置をとることができる。

【0135】

さらに、全パケットについて、振り分けられた種別毎に通信量をモニタしているため、当該情報を用いて、正常なパケットの通信のための適切な帯域を確保することもできる。

【図面の簡単な説明】

【0136】

【図 1】 図 1 は、本実施形態の iSCSI パケットを説明するための図である。

【図 2】 図 2 は、本実施形態のストレージシステムの機能構成図である。

【図 3】 図 3 は、本実施形態の LU アクセス許可テーブルを説明するための図である。

。

【図 4】 図 4 は、本実施形態の通信障害判定用閾値テーブルを説明するための図である。

【図 5】 図 5 は、本実施形態の通信ログを説明するための図である。

【図 6】 図 6 は、本実施形態において、記憶装置がパケットを受信した際の処理の流れを説明するための図である。

【図 7】 図 7 は、本実施形態のストレージシステムにおいて、不適切なパケットを受信した場合の処理フローである。

【図 8】 図 8 は、本実施形態の管理サーバにおける性能低下防止処理の処理フローである。

【図 9】 図 9 は、本実施形態の管理サーバにおける帯域制御処理の処理フローである。

。

【符号の説明】

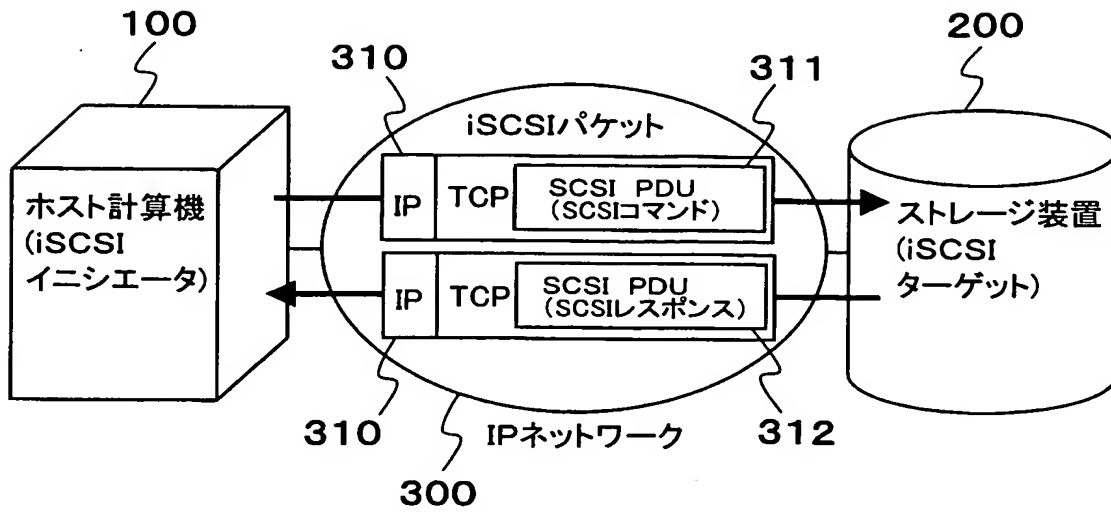
【0137】

100…記憶装置、110…ストレージ用インタフェース、111…制御プロセッサ、112…制御メモリ、113…不揮発メモリ、114…ポート、115…IP レベルフィルタ

タ部、116…LUレベルフィルタ部、117…通信量測定・判定部、118…通信情報
および障害通知部、119…iSCSI処理エンジン、121…LUアクセス許可テー
ブル、122…通信障害判定用閾値テーブル、130…論理ユニット、131…記憶領域制
御装置、150…保守用端末、151…制御プロセッサ、152…制御メモリ、153…
保守用端末記憶領域、154…インタフェース、155…インタフェース、156…通信
情報記録部、157…警告メッセージ通報部、158…通信ログ、161…通信制御部、
162…キャッシュメモリ、200…ホスト計算器、201…制御プロセッサ、202…
制御メモリ、203…I/F、211…iSCSIドライバ、300…IPネットワーク
、310…iSCSIパケット、311…SCSIコマンド、312…SCSIレスポ
ンス、320…ルータまたはスイッチ、400…管理サーバ、401…制御プロセッサ、4
02…制御メモリ、403…I/F、404…I/F、405…入力装置、406…出力
装置、411…帯域条件指定部、412…障害情報表示部、413…不正通信元解析部、
414…ルータ・スイッチ制御指示部、

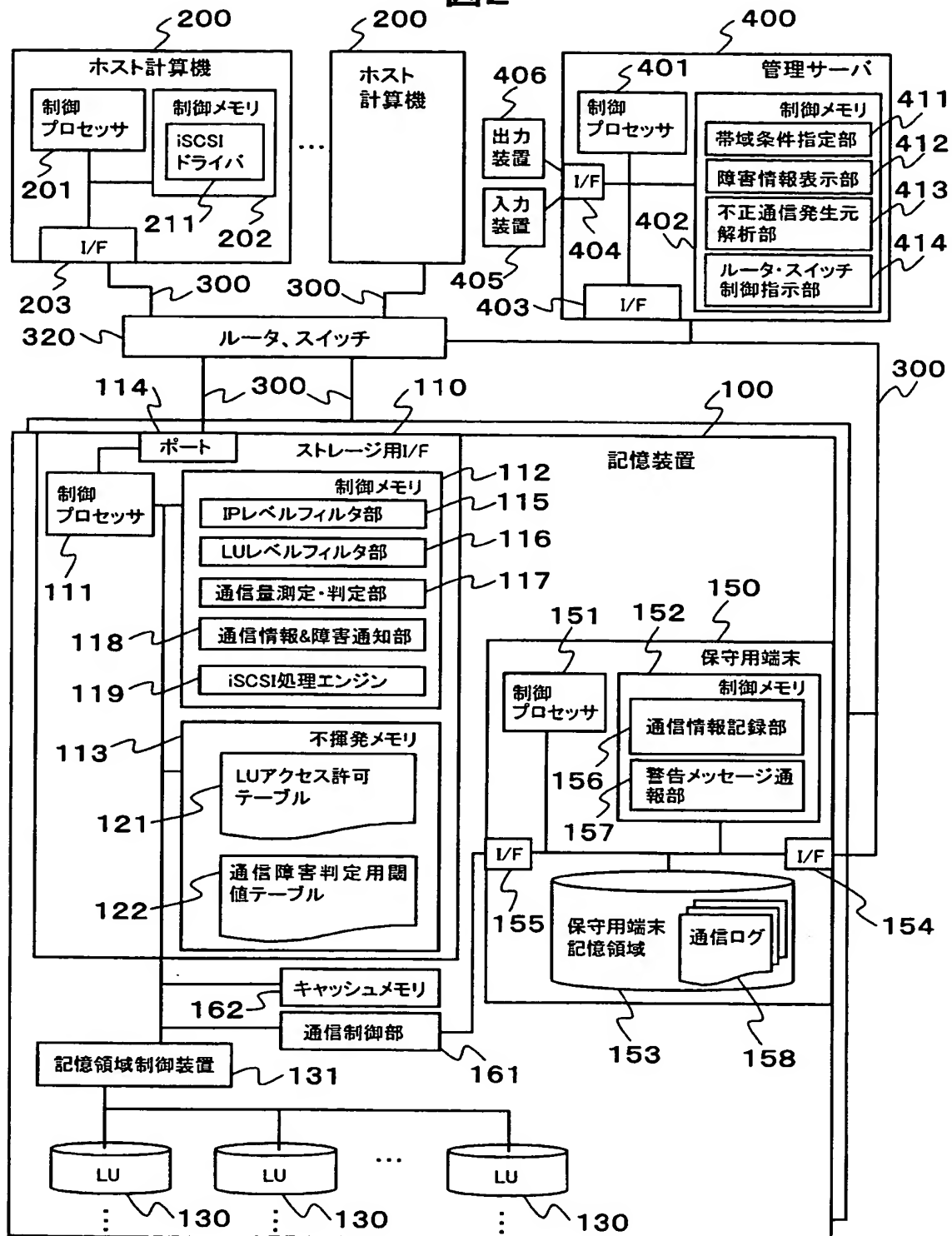
【書類名】 図面
【図 1】

図 1



【図 2】

図2



【図 3】

図3

1211 ⚡ iSCSIネーム	1212 ⚡ 仮想LUN	1213 ⚡ LUN
lqn.2003-07.com.XXX:iscsi-disk:mdel-YYY:sn-ZZZ	0,1,2,3,4	0,1,6,8,15
lqn.2003-07.com.RRR:iscsi-disk:mdel-SSS:sn-TTT	0,1,2	2,7,10
lqn.2003-07.com.OOO:iscsi-disk:mdel-PPP:sn-QQQ	0,1,2,3	3,4,5,14
⋮	⋮	⋮

⚡
121

【図 4】

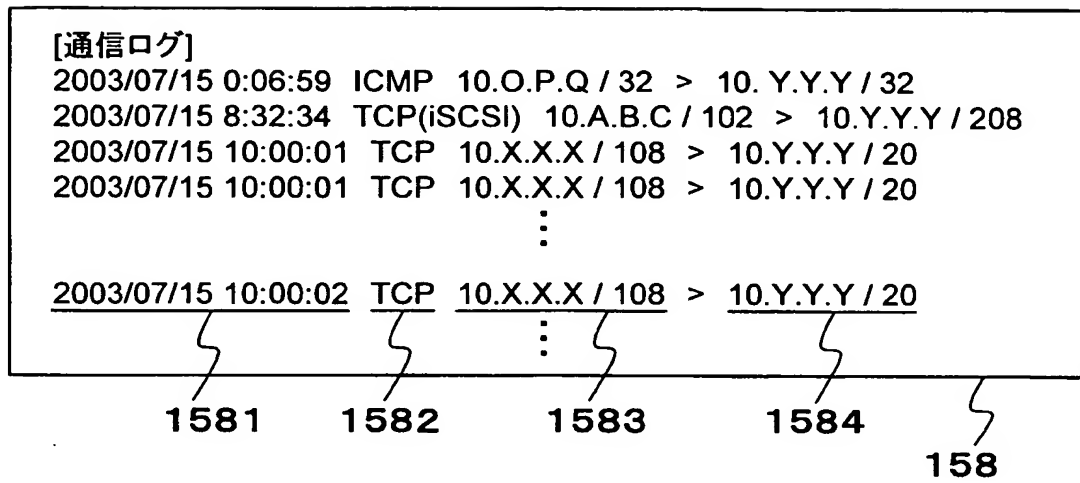
図4

122a ⚡	判定対象通信比	122b ⚡ 閾値
1221 ⌋	非iSCSI/パケット通信量(/S) / 全通信量(/S)	50%以上
1222 ⌋	不許可iSCSI/パケット通信量(/S) / iSCSI/パケット全通信量(/S)	30%以上
1223 ⌋	許可iSCSI/パケット通信量(/S) / 全通信量(/S)	60%以下
	⋮	⋮

⚡
122

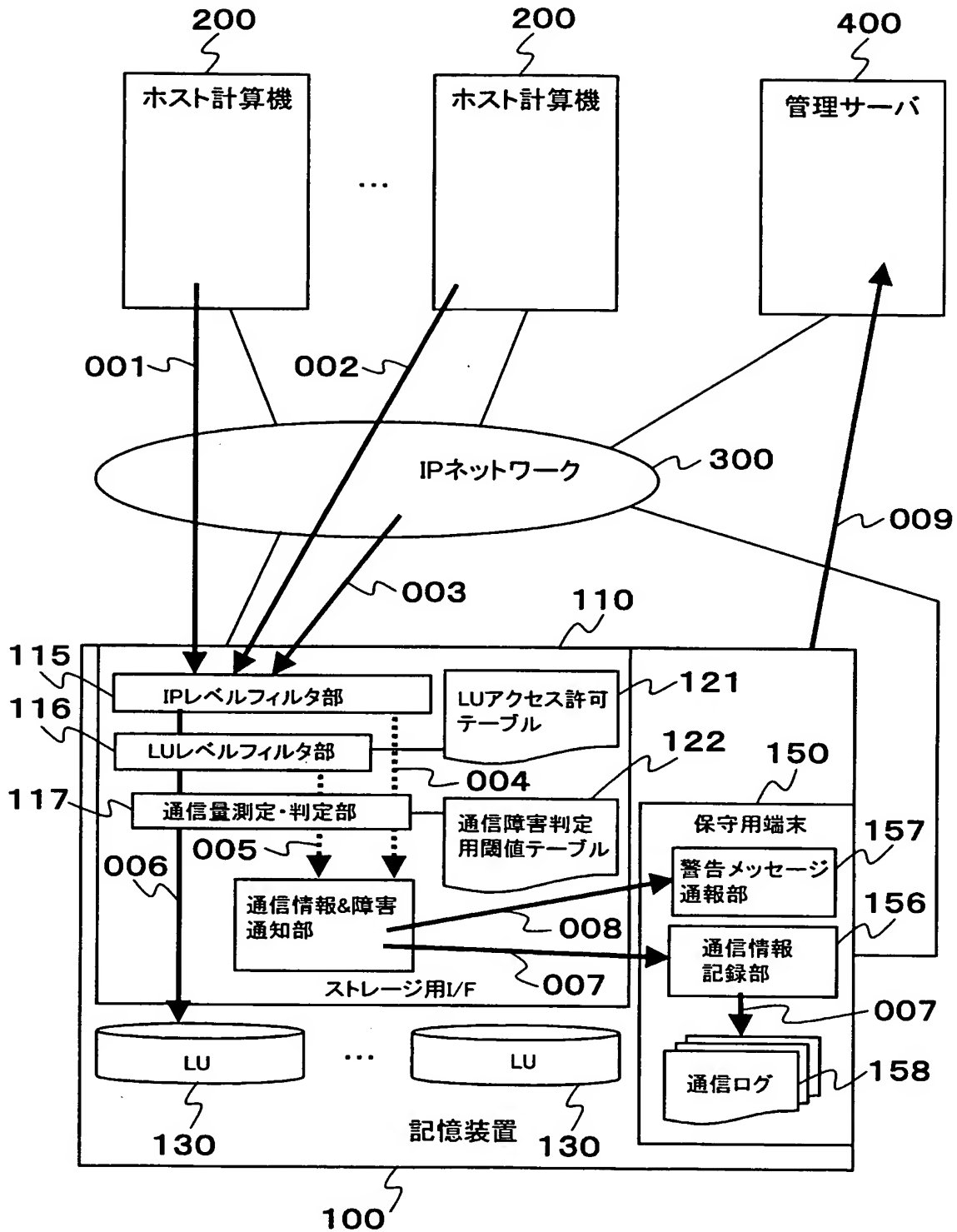
【図 5】

図5



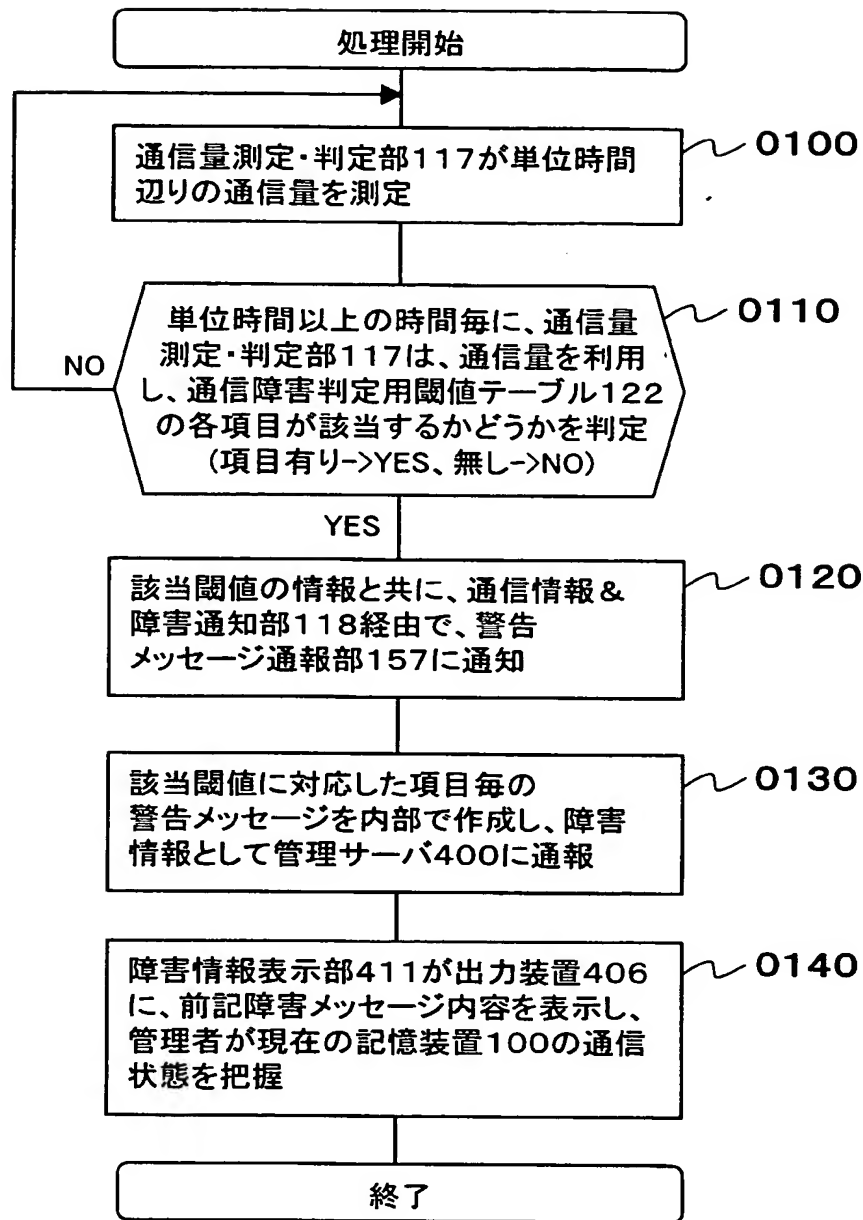
【図 6】

図 6



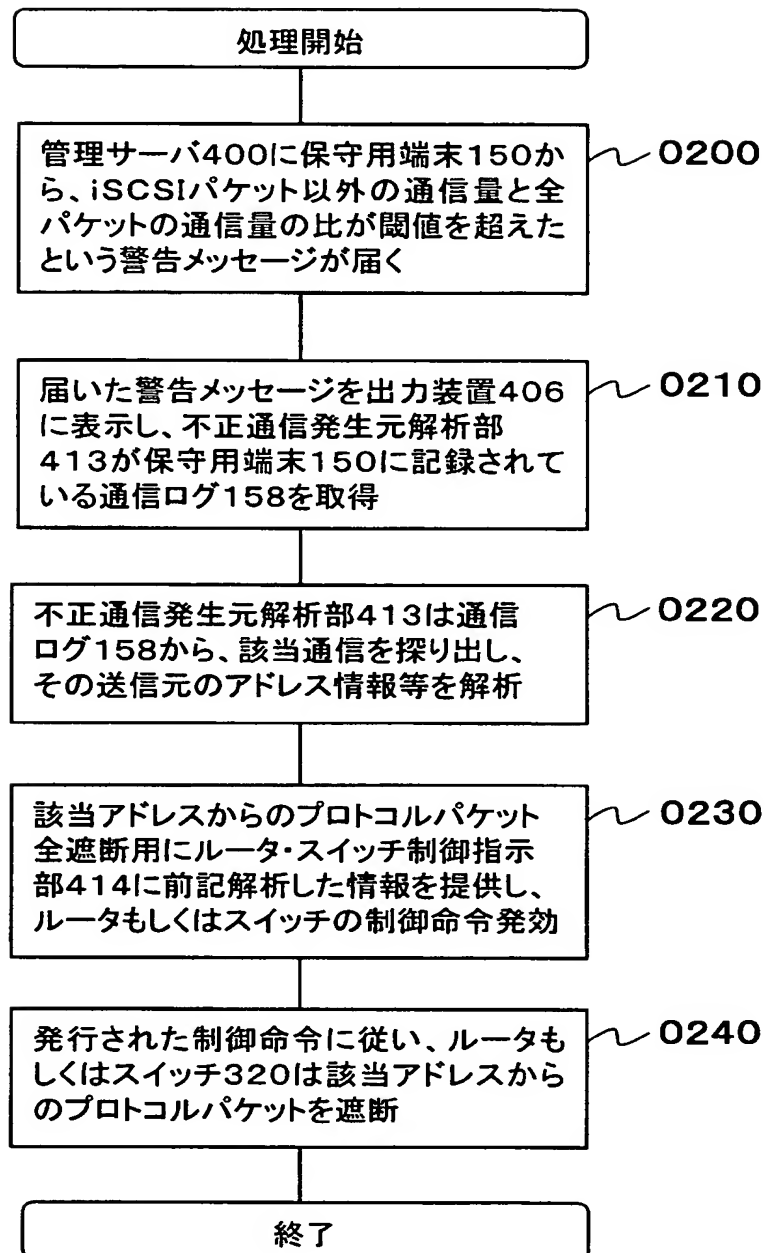
【図 7】

図 7



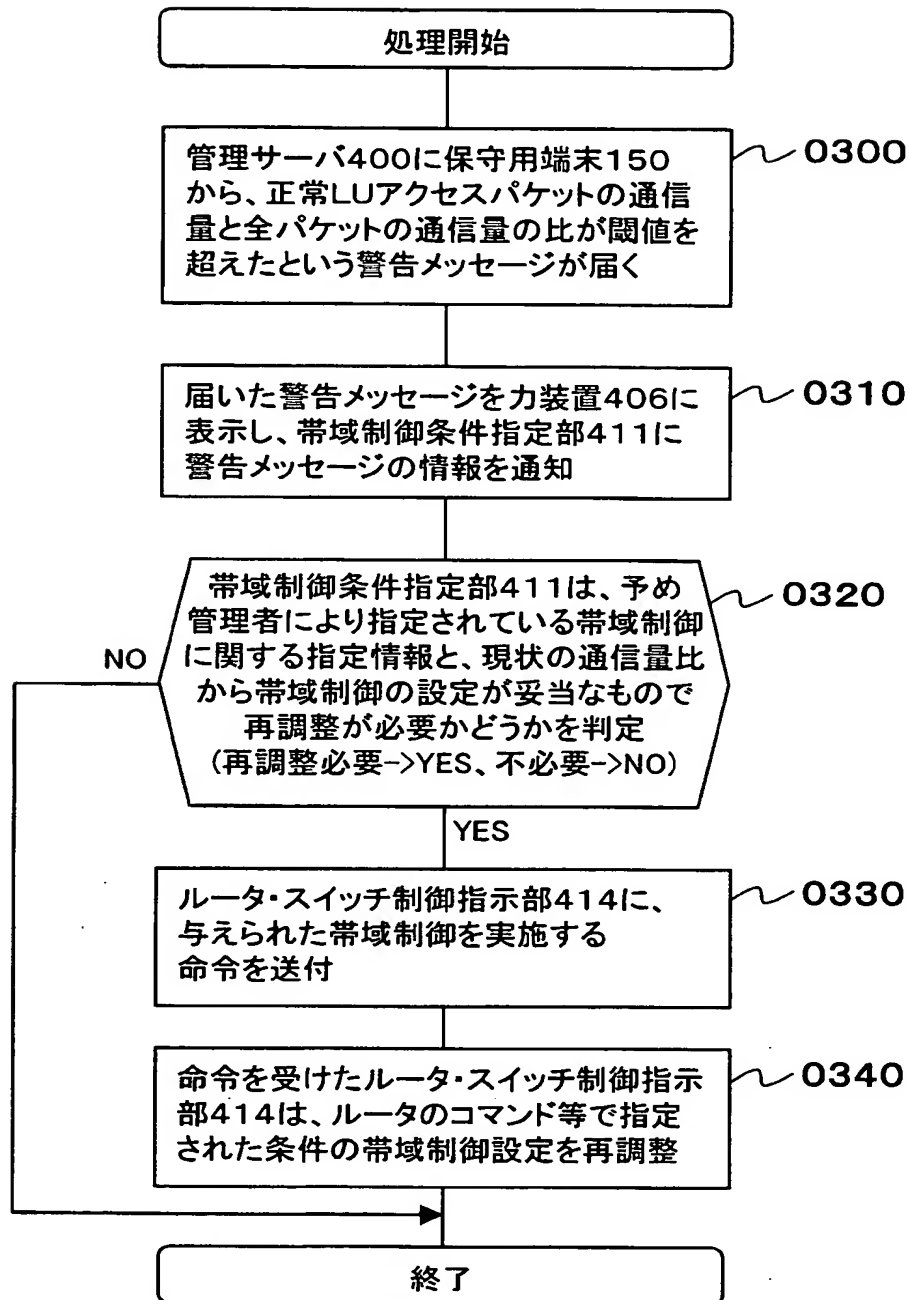
【図 8】

図8



【図 9】

図 9



【書類名】 要約書**【要約】****【課題】**

IP ネットワークに接続された記憶装置において、不正なパケットを排除することによりセキュリティを高めるとともに、記憶装置の論理ユニットへの通信性能を維持確保する。

【解決手段】

記憶装置内に、iSCSI パケット以外のパケットをフィルタリングする機能を備える。当該機能を通してのもののみ、論理ユニットへのアクセスの可否をフィルタリングする。

また、受信した全てのパケット、および、上記の2つのフィルタリング機能で振り分けられた各パケットごとの通信量を測定するとともに上記フィルタリングで廃棄扱いとなったパケットの通信ログを記録する。これらの情報を用いて、不正通信の遮断処理、正常通信のための帯域確保などの制御を行う。

【選択図】 図 2

特願 2 0 0 3 - 3 8 9 4 7 5

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 1 0 8]

1. 変更年月日	1 9 9 0 年 8 月 3 1 日
[変更理由]	新規登録
住 所	東京都千代田区神田駿河台 4 丁目 6 番地
氏 名	株式会社日立製作所